A TRIDENT SCHOLAR PROJECT REPORT

NO. 449

Construction of Rational Maps on the Projective Line with Given Dynamical Structure

by

Midshipman 1/C Ian E. Shaw, USN

UNITED STATES NAVAL ACADEMY
ANNAPOLIS, MARYLAND

USNA-1531-2

U.S.N.A. --- Trident Scholar project report; no. 449 (2016)

Construction of Rational Maps on the Projective Line with Given Dynamical Structure

by

Midshipman 1/C Ian E. Shaw
United States Naval Academy
Annapolis, Maryland

_____
(signature)

Certification of Advisers Approval

Associate Professor Amy Ksir
Mathematics Department

_____
(signature)

_____
(date)

LT Brian Stout, USN
Mathematics Department

_____
(signature)

_____
(date)

Acceptance for the Trident Scholar Committee

Professor Maria J. Schroeder
Associate Director of Midshipman Research

_____
(signature)

_____
(date)

USNA-1531-2

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-11-2016		

4. TITLE AND SUBTITLE
Construction of Rational Maps on the Projective Line with Given Dynamical Structure

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Shaw, Ian E.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Naval Academy
Annapolis, MD 21402

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
Trident Scholar Report no. 449 (2016)

12. DISTRIBUTION / AVAILABILITY STATEMENT

This document has been approved for public release; its distribution is UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In this paper we prove that we can construct a unique quadratic rational map on the projective line if given three fixed points and a pair of period two points. There are restrictions on the given points related to maintaining distinct existence of the fixed and periodic points.

We construct the quadratic rational map by focusing on the case of fixed points at 0, 1, ∞. In this space we use a Grobner basis to solve a system of equations formed by the coefficients of fixed point polynomials. The solution to this system is the set of coefficients of the quadratic rational map. Using a Mobius transformation, we can send any three distinct, desired fixed points to 0, 1, ∞, construct the map, and use an inverse Mobius transformation to bring the map to the original fixed points. As an application we discuss constructing certain elliptic curves via Lattes maps.

15. SUBJECT TERMS
Arithmetic Dynamics, Periodic Points, Rational Map

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**		43	**19b. TELEPHONE NUMBER** *(include area code)*

Construction of Rational Maps on the Projective Line with Given Dynamical Structure

Midshipman Ian Shaw, USN

Advisors: Professor Amy Ksir, Lieutenant Brian Stout, USN

United States Naval Academy

May 3, 2016

Abstract

In this paper we prove that we can construct a unique quadratic rational map on the projective line if given three fixed points and a pair of period two points. There are restrictions on the given points related to maintaining distinct existence of the fixed and periodic points.

We construct the quadratic rational map by focusing on the case of fixed points at $0, 1, \infty$. In this space we use a Gröbner basis to solve a system of equations formed by the coefficients of fixed point polynomials. The solution to this system is the set of coefficients of the quadratic rational map. Using a Möbius transformation, we can send any three distinct, desired fixed points to $0, 1, \infty$, construct the map, and use an inverse Möbius transformation to bring the map to the original fixed points.

As an application we discuss constructing certain elliptic curves via Lattès maps.

Keywords: Arithmetic Dynamics, Periodic Points, Rational Map

Contents

1. Introduction

The is a paper in arithmetic dynamics, a relatively young field at the intersection of the older studies of number theory and dynamical systems.

Dynamical systems are mathematical models for systems that change over time in a deterministic way. The simplest way to model such a system is with a set S of possible states of the system, and a function $\phi : S \to S$ describing what happens to each state after one unit of time. For example, S might represent the possible positions and velocities of a planet in the solar system; if S represents the position and velocity today, $\phi(S)$ would give the position and velocity tomorrow. The sequence of values $S, \phi(S), \phi(\phi(S)), \phi(\phi(\phi(S)))$ is called (inspired by this example) the orbit of S. Here the discrete units of time correspond to days.

A natural question to ask is what the long term behavior of the system will be. For some initial states, the planet will stay near the sun, and for others it will fly off into space and never return. Thus the principal goal of dynamics is to "classify the points α in the set S according to the behavior of their orbits $\mathcal{O}_\phi(\alpha)$." [3] We will use this goal in order to frame our investigation.

The set S in which we will work is not the set of positions of planets but rather the set of rational numbers. The orbits $\mathcal{O}_\phi(\alpha)$ we will be using are those forward orbits of a rational number α under repeated evaluation by a rational map.

Many advances in dynamical systems have been made since computers became available. The exponentially increased computational power and access to larger data sets rocketed the field forward, allowing mathematicians to observe phenomena on the smallest scale and over many iterations. The popular term, "butterfly effect", describes the fact that for many systems, a very small change in the initial state can be magnified to cause huge changes in long term behavior. The name was coined by Edward Lorenz, and comes from the idea that the flap of a butterfly's wings could change the path of a hurricane several weeks later. Lorenz pioneered the study of such systems, often called chaos theory, in the 1960's. Another popular advancement in dynamical systems spurred by the classification of points by their orbits was the development of beautiful and fascinating sets called fractals.

In the past few decades two pillars of theoretical mathematics, number theory and dy-

namical systems, have come together to create a new field: arithmetic dynamics. Relative to the study of mathematics as a whole, arithmetic dynamics is a frontier begging to be explored. Here we bring together a classical question from dynamical systems and the tools of number theory to take steps into this frontier. Can a function be developed in which a designated set of points has a designated behavior?

Specifically we deal with rational maps as the function, rational numbers as the points, and prime periodicity as the designated behavior. This project will investigate the uniqueness and existence of a rational map for a set of points of period 2, those points that reappear every other iteration of the map.

The central question of this paper is: Can we construct a quadratic rational map if given three fixed points and a pair of period two points? We have found the answer to be yes, with some restrictions on the fixed points and period two points. This question is motivated by a connection to the torsion points of elliptic curves.

As elliptic curve cryptography becomes more applicable in the information age, improving the central cryptosystem algorithm is of increasing importance. Part of this cryptosystem is being able to construct elliptic curves with certain characteristics; among these being specified torsion points. Joseph Silverman showed that there is a connection between the torsion points of an elliptic curve and the pre-periodic points of a Lattès map, a special type of rational map. We hope that we can construct a Lattès map with prescribed pre-periodic points and then determine elliptic curves with desired torsion points.

Thus we are interested in constructing rational maps with given pre-periodic points. This paper focuses on the case of quadratic rational maps in hopes of progressing to the more complex case of Lattès maps, which are maps of degree four or higher.

There are further related questions that have been asked by other researchers in this community. For example, consider points for which the first derivative of the map is zero, known as critical points. It is now known, thanks to a collection of mathematicians publishing in 2013 the paper "On the Classification of Critically Fixed Rational Maps," the classifications of rational maps for which all critical points are fixed. For example, for all degrees three or higher there exists a rational map such that all but two of the fixed points are critical[1]. Additionally, an active area of current research includes "post-critically finite maps" where

all critical points are preperiodic. That is to say, the research into categories of points on rational maps has been, and continues to be, investigated

The structure of this paper is as follows. In Section 2 we will elaborate upon our terms and notation. In Section 3 we will prove,by construction, the existence of quadratic rational maps with almost any specified two-cycle and fixed points at $0, 1, \infty$ by construction. In Section 4 we prove uniqueness of the quadratic rational map. In Section 5 we prove how to extend our conclusions for quadratic rational maps with fixed points at $0, 1, \infty$ to quadratic rational maps with any distinct fixed points and two-cycle. In Section 6 we discuss how these results relate to the bijection of the moduli 2-space of quadratic rational maps to the affine space. In Section 7 we explain the conclusions of the theorems through an example of a quadratic rational map. Finally in Section 8 we discuss the next steps in this research toward the goal of constructing elliptic curves with specified torsion points.

2. Background

The space we work in for this paper is known as the projective line.

Definition 2.1. The *projective line*, denoted by $\mathbb{P}^1$, is the rational numbers $\mathbb{Q}$ adjoined with the point at infinity ∞.

$$\mathbb{P}^1 = \mathbb{Q} \cup \{\infty\}$$

2.1. Rational Maps

Definition 2.2. A *rational map* is the quotient of two polynomials $a(x), b(x)$.

$$\phi(x) = \frac{a(x)}{b(x)} = \frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}{b_m x^m + b_{m-1}x^{n-1} + \cdots + b_1 x + b_0}$$

Definition 2.3. The *degree of a rational map* is the degree of the highest order term in the numerator or denominator.

In this paper, we are mostly concerned with maps of degree 2, also known as quadratic maps. These maps, unlike maps of degree one, have interesting and non-trivial iterates. For example, if ϕ is of degree 2, then $\phi \circ \phi = \phi^2$ is a degree 4 map. This opens the possibility for the conclusions we draw for quadratic maps to be extended to higher orders. The general form of a quadratic rational map is:

$$\phi(x) = \frac{a_2 x^2 + a_1 x + a_0}{b_2 x^2 + b_1 x + b_0} \tag{1}$$

An example of a quadratic rational map is:

$$g(x) = \frac{x^2 - 1}{x^2 - 2x + 1}.$$

2.2. Resultant

Not only are we interested in quadratic maps, but we do not want the rational maps to degenerate and become of smaller degree. To ensure the map maintains its degree we use a well known mathematical tool, the resultant of a rational map.

Theorem 1. *Let*

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

$$b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

be polynomials of degrees n and m with coefficients in a field K. There exists a polynomial

$$Res(a,b) = Res(a_n, \ldots, a_0, b_n, \ldots, b_m) \in \mathbb{Z}[a_n, \ldots, a_0, b_n, \ldots, b_m]$$

in the coefficients of $a(x)$ and $b(x)$, called the resultant of $a(x)$ and $b(x)$ with the following properties:

(a) Res (a,b)= 0 if and only if $a(x)$ and $b(x)$ have a common zero in $\mathbb{P}^1$

(b) The resultant is equal to the $(m+n)\times(m+n)$ determinant:

$$Res(a,b) = \begin{vmatrix} a_n & a_{n-1} & \ldots & a_0 & & & & \\ & a_n & a_{n-1} & \ldots & a_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & a_n & a_{n-1} & \ldots & a_0 & \\ b_m & b_{m-1} & \ldots & \ldots & b_0 & & & \\ & b_m & b_{m-1} & \ldots & b_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & & b_m & b_{m-1} & \ldots & b_0 \end{vmatrix}$$

Proof. See [3]. □

This is not well defined. Suppose α is a rational number and d is an integer, then

$$\mathrm{Res}(\alpha\phi) = \mathrm{Res}(\phi)\alpha^d.$$

Although it is not well defined, the vanishing of this polynomial is well defined. Suppose $\mathrm{Res}(\phi) = 0$, then $\mathrm{Res}(\alpha\phi) = 0$,

In this paper, if $\phi(x) = \frac{a(x)}{b(x)}$ is a quadratic rational map, then $\mathrm{Res}(\phi) = \mathrm{Res}(a,b)$. Therefore, the resultant may be used to determine whether the numerator and denominator have a common factor, causing ϕ to degenerate. In the quadratic case the resultant is

$$\mathrm{Res}(a,b) = \mathrm{Res}(\phi) = \begin{vmatrix} a_2 & a_1 & a_0 & 0 \\ 0 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 \\ 0 & b_2 & b_1 & b_0 \end{vmatrix}.$$

Returning back to the example of g:

$$\mathrm{Res}(g) = \begin{vmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{vmatrix} = 0.$$

Thus we see $g(x)$ must degenerate from a quadratic. Taking another look :

$$g(x) = \frac{x^2 - 1}{x^2 - 2x + 1} = \frac{(x-1)(x+1)}{(x-1)^2} = \frac{(x+1)}{(x-1)}$$

we see that $g(x)$ is in fact a linear map.

Consider another map:

$$h(x) = \frac{x^2 + 1}{x^2 - 2x + 1}.$$

$$\mathrm{Res}(h) = \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{vmatrix} = 4$$

We see that $h(x)$ does not degenerate, and is in fact quadratic.

2.3. Periodic Points

Now let's take a look at interesting points in this space. Consider an $\alpha \in \mathbb{P}^1(\mathbb{Q})$.

Definition 2.4. If there is a $n \in \mathbb{Z}^+$ such that $\phi^n(\alpha) = \alpha$, then α has period n, also is called a *periodic point*.

Definition 2.5. If $\phi(\alpha) = \alpha$, then α is a point of period one, also known as a *fixed point*.

If $\phi^2(\alpha) = \alpha$, then α is a point of period two. Furthermore, $\phi(\alpha)$ is a point of period two.

$$\phi^2(\phi(\alpha)) = \phi(\phi(\phi(\alpha))) = \phi(\phi^2(\alpha)) = \phi(\alpha)$$

Then $\alpha, \phi(\alpha)$ are said to form a two-cycle as the maps send the points to each other; $\alpha \rightleftharpoons \phi(\alpha)$, and more over $\alpha, \phi(\alpha)$ are distinct.

One of the standard questions in dynamical systems is to find the fixed points and periodic points of the system. The number of possible periodic points of a given period depends on the degree of the map. We can see this by studying the fixed point polynomial.

Definition 2.6. If x is a fixed point, then $\phi(x) = \frac{a(x)}{b(x)} = x$. The *fixed point polynomial of* ϕ is $\text{Fix}_\phi(x) = a(x) - xb(x)$.

Lemma 2. *If the point* α *is a fixed point of* ϕ*, then* $Fix_\phi(\alpha) = 0$

Proof. Let α be a fixed point of ϕ.

$$\phi(\alpha) = \frac{a(\alpha)}{b(\alpha)} = \alpha$$

By simple distribution,

$$0 = a(\alpha) - \alpha b(\alpha)$$

Thus $\text{Fix}_\phi(\alpha) = 0$.

□

Consider the fixed point polynomial of the general quadratic rational map. Let x be a general fixed point of ϕ.

$$\phi(x) = \frac{a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + b_0}$$

Let f_n denote a single fixed point.

$$0 = \phi(x) - x = a(x) - xb(x) = a_2x^2 + a_1x + a_0 - b_2x^3 + b_2x + b_1 = (x - f_1)(x - f_2)(x - f_3)$$

As you can see, for a quadratic rational map there are at most three fixed points.

Consider the same ϕ. The second iterate of ϕ will be a quartic rational map

$$\phi^2(x) = \phi(\phi(x)) = \frac{A(x)}{B(x)}$$

where $A(x), B(x)$ are degree 4 polynomials in terms of the coefficients of $\phi : a_2, a_1, a_0, b_2, b_1, b_0$ This new map will maintain the fixed points f_1, f_2, and f_3. Let p_n be period two points of ϕ. For ϕ^2, period two points of ϕ will be become fixed points.

$$\phi^2(f_1) = \phi(\phi(f_1)) = \phi(f_1) = f_1$$

$$\phi^2(p_n) = p_n$$

The fixed point polynomial will be a degree 5 polynomial.

$$0 = \phi^2(x) - x = A(x) - xB(x) = (x - f_1)(x - f_2)(x - f_3)(x - p_1)(x - p_2)$$

Since degree 5, there are five roots. Since three are already fixed points, we see that a quadratic rational map can have at most two period-two points. Note that since by definition $\phi(p_1)$ is a period 2 point of ϕ, that $p_2 = \phi(p_1)$. For this paper, we will be concerned with constructing quadratic rational maps based off conditions of a given set of three fixed points and two period-two points.

2.4. Simplifying the General Quadratic Rational Map

The goal of this paper is to construct a unique quadratic rational map. This may be understood as finding values for the coefficients $a_2, a_1, a_0, b_2, b_1, b_0$. These values are what narrow the scope of the general form of the quadratic rational map to adopt the specific fixed points and period two points we desire.

One way we simplify our calculations is by focusing on maps with fixed points $0, 1, \infty$. This is mathematically viable as it is known that for any distinct three points, there is a Möbius transformation sending these points to any other set of three distinct points [3]. Therefore we may work under the convenient conditions of fixed points of the map as 0, 1, ∞ with the understanding that our conclusions may be transformed to any three distinct fixed points f_1, f_2, f_3.

Consider a quadratic rational map with fixed points 0,1, ∞. Since 0 is a fixed point, then a_0 must equal to 0.

$$\frac{a_2 \cdot 0^2 + a_1 \cdot 0 + a_0}{b_2 \cdot 0^2 + b_1 \cdot 0 + b_0} = \frac{a_0}{b_0} = 0$$

Since ∞ is a fixed point, then b_2 must be equal to 0.

$$\frac{a_2 \cdot \infty^2 + a_1 \cdot \infty + a_0}{b_2 \cdot \infty^2 + b_1 \cdot \infty + b_0} = \frac{a_2}{b_2} = \infty$$

This results in a quadratic rational map with only four unknown coefficients, as opposed to the six we began with.

$$\frac{a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + b_0} \Rightarrow \frac{a_2x^2 + a_1x}{b_1x + b_0}$$

Since 1 is a fixed point we develop a condition upon the remaining coefficients.

$$\phi(1) = 1 = \frac{a_2 + a_1}{b_1 + b_0}$$

$$a_2 + a_1 = b_1 + b_0$$

Also note that if $a_2 = 0$ or $b_0 = 0$ the map will become linear. Therefore if a quadratic rational map ϕ has fixed points 0,1, ∞, then

$$\phi(x) = \frac{a_2x^2 + a_1x}{b_1x + b_0} \text{ such that } a_2, b_0 \neq 0 \text{ and } a_2 + a_1 = b_1 + b_0.$$

3. Existence by Construction

3.1. Existence Theorem

Theorem 3. *Let p, q be distinct rational numbers. There exists a quadratic rational map with fixed points 0,1, ∞ and p, q as a distinct two cycle if and only if p, q satisfy the following conditions:*

$$\{p + q \neq 0, p + q - 2 \neq 0, 2pq - p - q \neq 0\} \qquad (*)$$

Proof. First we will prove the forward direction with a provided quadratic map using algebra to show the fixed points and two-cycle hold for the map, then using the resultant to show that the map is quadratic and does not degenerate. The reverse direction will use a proof by contradiction to show that if any of the conditions are not met, then the quadratic map does not exist.

Suppose p, q satisfy the conditions of the theorem. Consider the map:

$$\phi(x) = \frac{(2pq - p - q)x^2 - (p^2q + pq^2 - p^2 - q^2)x}{(p^2 + q^2 - p - q)x - pq(p + q - 2)}$$

The point 0 is a fixed point by inspection. The point at ∞ is a fixed point since when the degree of a map is greater in the numerator than the denominator, then $\phi(\infty) = \infty$. The point 1 is a fixed point as shown below.

$$\phi(1) = \frac{(2pq - p - q) - (p^2q + pq^2 - p^2 - q^2)}{(p^2 + q^2 - p - q) - pq(p + q - 2)} = \frac{-1 \cdot (p - 1)(q - 1)(p + q)}{-1 \cdot (p - 1)(q - 1)(p + q)} = 1$$

The map at p and q forms a two cycle.

$$\phi(p) = \frac{(2pq - p - q)p^2 - (p^2q + pq^2 - p^2 - q^2)p}{(p^2 + q^2 - p - q)p - pq(p + q - 2)} = \frac{q(-p + q) \cdot p \cdot (p - 1)}{(-p + q) \cdot p \cdot (p - 1)} = q$$

$$\phi(q) = \frac{(2pq - p - q)q^2 - (p^2q + pq^2 - p^2 - q^2)q}{(p^2 + q^2 - p - q)q - pq(p + q - 2)} = \frac{p(p - q) \cdot q \cdot (q - 1)}{(p - q) \cdot q \cdot (q - 1)} = p$$

We will use the resultant of $\phi(x)$ to prove it is quadratic.

$$\text{Res}(\ \phi(x)\ ) = \begin{vmatrix} (2pq - p - q) & (p^2q + pq^2 - p^2 - q^2) & 0 & 0 \\ 0 & (2pq - p - q) & (p^2q + pq^2 - p^2 - q^2) & 0 \\ 0 & (p^2 + q^2 - p - q) & pq(p + q - 2) & 0 \\ 0 & 0 & (p^2 + q^2 - p - q) & pq(p + q - 2) \end{vmatrix}$$

$$= (-1) \cdot q \cdot (q-1) \cdot p \cdot (p-1) \cdot (p+q) \cdot (p+q-2) \cdot (-p+q)^2 \cdot (2pq-p-q)$$

As discussed in Section 2.2 We assumed 0, 1, p, q are all distinct and therefore p, q, $(q-1)$, $(p-1)$, $(-p+q)$ are all non-zero. Together with the conditions (*), the resultant of ϕ is not 0. Therefore the numerator and denominator of ϕ do not have a common root. Since ϕ is of degree two, it is quadratic.

Now suppose that there is a quadratic rational map with fixed points 0, 1, ∞ and p, q as a distinct two cycle.

As discussed in Section 2.4, such a map must take the form:

$$\phi(x) = \frac{a_2x^2 + a_1x}{b_1x + b_0} \text{ such that } a_2, b_0 \neq 0 \text{ and } a_2 + a_1 = b_1 + b_0.$$

We will refer to $0 = a_2 + a_1 - b_1 - b_0$ as the $\phi(1)$ equation. By definition, since 1 and 0 are fixed points, they are not period 2 points. We want to show that the values p, q satisfy the conditions (*). For the three conditions we will use a proof by contradiction. We will assume that $\phi(x)$ is a quadratic rational map and one of the conditions is not met, then show that $a_2 = 0$ or $b_0 = 0$. This causes $\phi(x)$ to reduce to a degree 1, non-quadratic map; creating a contradiction.

Case 1. *Suppose* $p + q = 0$.

Since $\phi(p) = q = -p$ and $\phi(q) = \phi(-p) = p$, the following equations are established.

$$\phi(p) = -p = \frac{a_2p^2 + a_1p}{b_1p + b_0} \Rightarrow 0 = a_2p^2 + a_1p - (-p)(b_1p + b_0)$$

$$\phi(-p) = p = \frac{a_2p^2 + a_1(-p)}{b_1(-p) + b_0} \Rightarrow 0 = a_2(p)^2 + a_1(-p) - p(b_1(-p) + b_0)$$

By adding the $\phi(p)$ and $\phi(-p)$ equations we find that

$$0 = 2p^2(a_2 + b_1).$$

Since $p \neq 0$ then $a_2 = -b_1$.

By subtracting the $\phi(p)$ and $\phi(-p)$ equations we find that

$$0 = 2p(a_1 + b_0).$$

Since $p \neq 0$ then $a_1 = -b_0$.

When we substitute these into the $\phi(1)$ equation we find that $b_1 = -b_0$.

Finally substituting for a_2, a_1, b_1 into the $\phi(p)$ equation it shows

$$0 = -1 \cdot p \cdot (p-1)b_0.$$

Since $p, 0$, and 1 are assumed to be distinct; $p, (p-1) \neq 0$. Therefore $b_0 = 0$.

Case 2. *Suppose* $p + q - 2 = 0$.

Since $\phi(p) = q = 2 - p$ and $\phi(q) = \phi(2-p) = p$, the following equations are established.

$$\phi(p) = 2 - p = \frac{a_2p^2 + a_1p}{b_1p + b_0} \Rightarrow 0 = a_2p^2 + a_1p - (2-p)(b_1p + b_0)$$

$$\phi(2-p) = p = \frac{a_2(2-p)^2 + a_1(2-p)}{b_1(2-p) + b_0} \Rightarrow 0 = a_2(2-p)^2 + a_1(2-p) - p(b_1(2-p) + b_0)$$

When subtracting the $\phi(p)$ from the $\phi(2-p)$ equation we find that

$$b_0 = -1 \cdot (2a_2 + a_1).$$

When substituting b_0 into the $\phi(1)$ equation we find the equation

$$b_1 = 3a_2 + 2a_1.$$

When b_1, b_0 are substituted back into the $\phi(p)$ equation we find that

$$0 = (4a_2 + 2a_1)(p-1)^2.$$

Since $p \neq 1$ then $0 = 4a_2 + 2a_1$. Thus $a_1 = -2a_2$. When this is substituted in the b_0 equation

$$b_0 = -1 \cdot (2a_2 + a_1) = -1 \cdot (2a_2 - 2a_2) = 0.$$

Case 3. *Suppose* $2pq - p - q = 0$.

Since $\phi(p) = q = \frac{p}{2p-1}$ and $\phi(q) = \phi(\frac{p}{2p-1}) = p$, the following equations are established.

$$\phi(p) = \frac{p}{2p-1} = \frac{a_2p^2 + a_1p}{b_1p + b_0} \Rightarrow p(b_1p + b_0) = (2p-1)(a_2p^2 + a_1p)$$

$$\phi(p) : 0 = -2a_2p^3 + a_2p^2 - 2a_1p^2 + b_1p^2 + a_1p + b_0p$$

$$\phi(\frac{p}{2p-1}) = p = \frac{a_2(\frac{p}{2p-1})^2 + a_1(\frac{p}{2p-1})}{b_1(\frac{p}{2p-1}) + b_0} \Rightarrow p(b_1(2p-1) + b_0(2p-1)^2) = a_2p^2 + a_1p(2p-1)$$

$$\phi(\frac{p}{2p-1}) : 0 = -2b_1p^3 - 4b_0p^3 + a_2p^2 + 2a_1p^2 + b_1p^2 + 4b_0p^2 - a_1p - b_0p.$$

By adding the $\phi(p)$ and $\phi(\frac{p}{2p-1})$ equations together we find that

$$0 = 2 \cdot (p-1)(a_2 + b_1 + 2b_0).$$

Since $p \neq 1$ then $0 = (a_2 + b_1 + 2b_0)$. Therefore $a_2 = -2b_0 - b_1$.
When this is substituted into the $\phi(p)$ equation we find that

$$a_1 = 2b_1 + 3b_0.$$

When substituting a_2, a_1 into the $\phi(\frac{p}{2p-1})$ equation, we find that

$$0 = 2p(p-1)^2(b_1 + 2b_0).$$

Since $p, (p-1) \neq 0$ then $2b_0 + b_1 = 0$. Therefore $b_1 = -2b_0$. This leads to the conclusion that

$$a_2 = -2b_0 - b_1 = -2b_0 + 2b_0 = 0.$$

We have shown that if each condition is not met, then $\phi(x)$ cannot be a quadratic rational map.
Therefore the forward and backward conditionals of the theorem have been proven. □

3.2. Geometric Explanation of Existence Theorem Conditions

The proof highlights the algebraic reasoning for the conditions on a rational map; this section addresses the geometric reasoning. Here again is the resultant of the rational map ϕ described in the proof.

$$\text{Res}(\phi(x)) = (-1) \cdot q \cdot (q-1) \cdot p \cdot (p-1) \cdot (-p+q)^2 \cdot (p+q) \cdot (p+q-2) \cdot (2pq-p-q)$$

We are concerned with conditions that cause the resultant to be zero, so the leading -1 is irrelevant. The next four terms are addressed by the condition "distinct two-cycle" for the rational map. The factors $q, (q-1), p, (p-1)$ ensure that the fixed points of 0 and 1 are not

also considered part of the two cycle. The next factor $(-p+q)$ ensures that the period two points are not the same, thus becoming a fixed point.

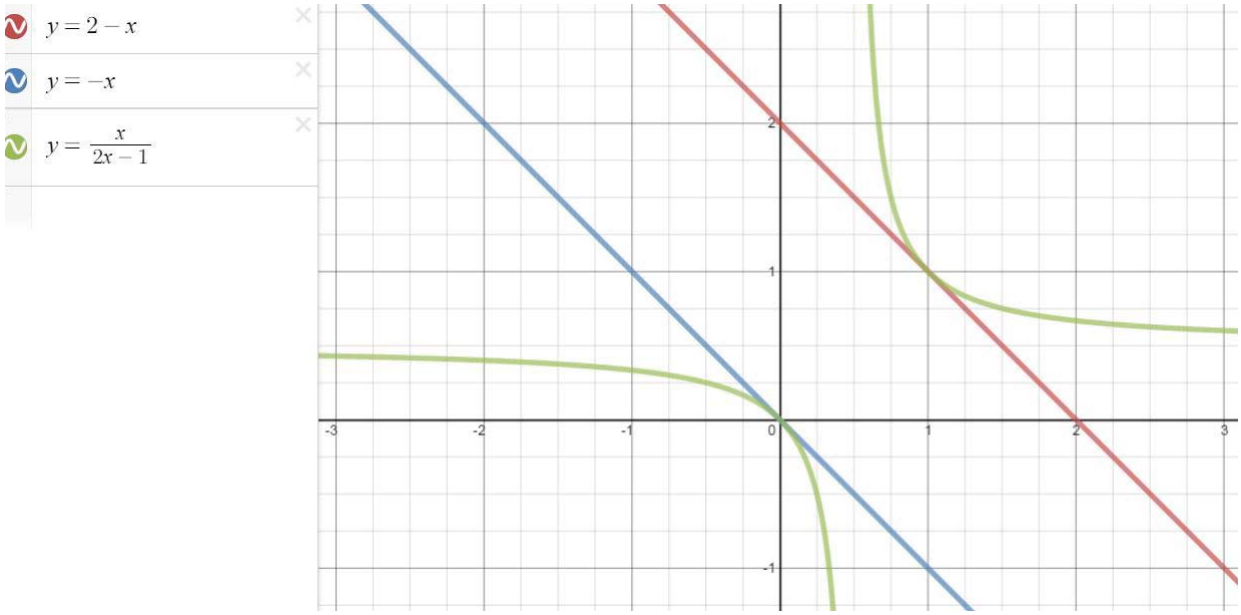
The final three terms are more interesting. Consider what happens to the map when these terms are set equal to 0:

$$\phi(x) = \frac{(2pq-p-q)x^2 - (p^2q+pq^2-p^2-q^2)x}{(p^2+q^2-p-q)x - pq(p+q-2)}$$

$$0 = (p+q-2) \Rightarrow q = 2-p \Rightarrow \phi(x) = 2-x \Rightarrow \phi(0) = 2$$

$$0 = (p+q) \Rightarrow q = -p \Rightarrow \phi(x) = -x \Rightarrow \phi(1) = -1$$

$$0 = (2pq-p-q) \Rightarrow q = \frac{p}{2p-1} \Rightarrow \phi(x) = \frac{x}{2x-1} \Rightarrow \phi(\infty) = \frac{1}{2}$$



Even though no longer quadratic, each two cycle is preserved. The trade off is that one of the fixed points disappears; leaving each map to be degree one with two fixed points and a two-cycle.

4. Uniqueness

4.1. Basics of Gröbner Bases

In our research we found a need to solve non-trivial systems of polynomial equations. In order to do so with the computer algebra system Sage, we used Gröbner bases. This section is focused on explaining the nature of Gröbner basis, first created by Bruno Buchberger and named after his advisor, Wolfgang Gröbner.

Our difficulties began with a system of equations that arise in our proof of a quadratic rational map's uniqueness. These equations may be organized into a set of polynomials with rational coefficients.

Definition 4.1. Let F be a finite set of polynomials in a polynomial ring $\mathbf{R}$. Let I be the set of linear combinations of elements from F with coefficients in all of $\mathbf{R}$. I is known as the *ideal generated by* F.

Example. Over the course of this section, we will refer to I to illustrate the theory.

$$I = \langle k_1, k_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$$

$$= \{(x^3 - 2xy)f(x,y) + (x^2y - 2y^2 + x)g(x,y)\}$$

Definition 4.2. Given an ideal $I = \langle k_1, k_2, \ldots k_n \rangle$, the polynomials k_n are called the *generators* of the ideal.

Ideals have many generating sets; a Gröbner basis is a certain type of generating set that facilitates solving systems of polynomial equations.

Important to the process of developing a Gröbner basis is the concept of *monomial ordering*; the way by which the the monomials are ordered within the polynomial ring. There are several types of ordering. One example of an ordering is degree lexicographic; this means the terms are listed in descending degree then alphabetical order. This ordering is often shortened to *deglex*. In our proof of Theorem 5 we use total degree reverse lexicographical ordering (also known as *degrevlex*) by which terms are listed in descending total degree then reverse ordered by the exponent of the last lexicographic term. Below is a comparison of the two types of monomial orderings applied to I.

$$\text{deglex: } I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$$

$$\text{degrevlex: } I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$$

You can see that the two polynomials remain the same.

Consider the following example ideal J, here the two monomial orderings do change the arrangement of the polynomials.

$$\text{deglex: } J = \langle x^4yz^2, xy^5z + x^2yz^3 + xy^4z \rangle$$

$$\text{degrevlex: } J = \langle xy^5z + xy^4z + x^2yz^3, x^4yz^2 \rangle$$

Interesting to note is that different choices of ordering ordering used for Buchberger's algorithm for constructing a Gröbner basis can result in different sizes of bases. For the proof of Theorem 5, the Gröbner basis contains 14 polynomials if calculations are started with a degrevlex ordering (Appendix A), but 35 polynomials if started with a lexicographic ordering. Thus we use the former for the sake of tractability.

Definition 4.3. The *leading term* of a polynomial k is the largest monomial term in the polynomial. This is dependent upon the choice of monomial ordering of the polynomial ring. This is denoted $\text{LT}(k)$.

The philosophy behind creating the Gröbner basis of an ideal is to eliminate variables. The ordering of the Gröbner basis determines the sequence of eliminating these variables. Referring to our example above, $\text{LT}(k_1)=x^3$ in both deglex and degrevlex orderings.

Definition 4.4. Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be a *Gröbner Basis* if

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle.$$

The word "basis" in Gröbner basis is a slight misnomer because the set of generators in a Gröbner basis need not be reduced to the minimum number of elements. For example, $y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2$ and thus $-x^2 \in I$ using the generators k_1, k_2; but we will see later that $-x^2$ is included among the generators of the Gröbner basis of I.

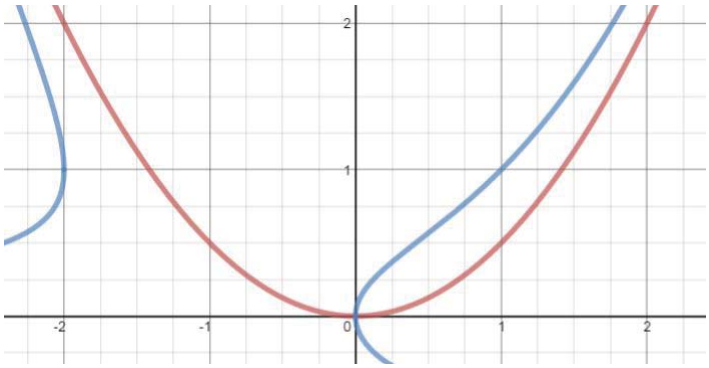


Figure 1: The graph of the the two polynomial equations.

4.2. Gröbner Basis Example

To illustrate the use of Gröbner bases, we will use an example. This will show how computing a Gröbner basis can be used to solve a system of polynomial equations.. The same concepts are used in the proof of Theorem 5.

Consider the system of two equations:

$$x^3 - 2xy = 0$$

$$x^2y - 2y^2 + x = 0$$

A solution to this system is a value of x and y simultaneously solving both equations. Visually this corresponds to the point of intersection in the graph. We can use a Gröbner basis to solve the system of two equations. Any (x, y) that is a solution to the original system wil also satisfy $f(x, y) = 0$ for any other $f \in I$.

Here we will use what is called *Buchberger's Algorithm* in order to find the the Gröbner basis of I [2]. This is a process of developing S-polynomials of generators, dividing the S-polynomials by the working set of polynomials, and adding the remainders to the working set until the set is Gröbner basis.

First we need a definition of the S-polynomial.

Definition 4.5. The *S-polynomial* of k and g is the combination

$$S(k, g) = \frac{r}{\mathrm{LT}(k)} \cdot k - \frac{r}{\mathrm{LT}(g)} \cdot g,$$

where r is the least common multiple of LT(k) and LT(g), therefore both $\frac{r}{\text{LT}(k)}$ and $\frac{r}{\text{LT}(g)}$ are both monomials in the polynomial ring.

First we will compute the S-polynomial of k_1 and k_2 in our example above.

$$S(k_1, k_2) = \frac{x^3y}{x^3} \cdot (x^3 - 2xy) - \frac{x^3y}{x^2y} \cdot (x^2y - 2y^2 + x) = -x^2$$

You can see that $-x^2$ is not divisible by LT(k_1) or LT(k_2). For the basis $K = \{k_1, k_2\}$ the remainder of the S-polynomial after division by K (denoted by $\overline{S(k_1, k_2)}^K$) is the same as the S-polynomial:

$$\overline{S(k_1, k_2)}^K = -x^2.$$

Therefore $K = \{k_1, k_2\}$ is not a Gröbner basis, as $-x^2 \in I$, but $x^2 \notin \langle \text{LT}(k_1), \text{LT}(k_2) \rangle = \langle x^3, x^2y \rangle$. Therefore we will add $-x^2$ to K and denote it by $k_3 = -x^2$; $K = \{k_1, k_2, k_3\}$. Now the remainder of the S-polynomial is zero among the basis K.

$$\overline{S(k_1, k_2)}^K = 0$$

Definition 4.6. A generating set $K = (k_1, k_2, \ldots k_n)$ is *closed* if

$$\overline{S(k_i, k_j)}^K = 0 \text{ for all } 1 \leq i \leq j \leq n.$$

We will continue this process of generating the S-polynomials from pairs of polynomials in our basis, and adding the remainders to the basis as necessary, until the basis is closed. Once closed, a generating set is considered a Gröbner basis. This qualification is also known as *Buchberger's criterion.* [2]

$$S(k_1, k_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy$$

$$\overline{S(k_1, k_3)}^K = -2xy$$

$$k_4 = -2xy$$

$$K = \{k_1, k_2, k_3, k_4) = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy\}$$

$$S(k_1, k_4) = y(x^3 - 2xy) - (\frac{-x^2}{2})(-2xy) = -2xy^2 = yk_4 \rightarrow \overline{S(k_1, k_4)}^K = 0$$

$$S(k_2, k_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x$$

$$\overline{S(k_2,k_3)}^K = -2y^2 + x$$

$$k_5 = -2y^2 + x$$

$$K = \{k_1, k_2, k_3, k_4, k_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

$$S(k_1,k_5) = -2y^3(x^3 - 2xy) - x^3(-2y^2 + x) = -x^4 + xy^3 = -k_3^2 + yk_4^2 \to \overline{S(k_1,k_5)}^K = 0$$

$$S(k_2,k_4) = -2(x^2y - 2y^2) - x(-2xy) = 4y^2 - 2x = -2k_5 \to \overline{S(k_2,k_4)}^K = 0$$

$$S(k_2,k_5) = -2y(x^2y - 2y^2) - x^2(-2y^2 + x) = -x^3 + 4y^3 - 2xy = xk_3 - 2yk_5 \to \overline{S(k_2,k_5)}^K = 0$$

$$S(k_3,k_4) = 2y(-x^2) - x(-2xy) = 0 \to \overline{S(k_3,k_4)}^K = 0$$

$$S(k_3,k_5) = 2y^2(-x^2) - x(-2y^2 + x) = -x^3 = xk_3 \to \overline{S(k_3,k_5)}^K = 0$$

$$S(k_3,k_4) = y(-2xy) - x(-2y^2 + x) = -x^2 = k_3 \to \overline{S(k_4,k_5)}^K = 0$$

We have shown that K is closed.

$$\overline{S(k_i,k_j)}^K = 0 \text{ for all } 1 \leq i \leq j \leq 5.$$

Thus K is the Gröbner basis for the ideal I.

Theorem 4. *Buchberger's Algorithm terminates.*

Proof. See [2]. □

Theorem 4 Gröbner bases always exist for any ideal starting with a generating subset. In general, the Gröbner basis is a large generating of simpler polynomials we can use to solve for the variables in the system of polynomial equations.

Since the Gröbner basis generates the ideal I, a solution to the system of equations,

$$k_1 = 0$$

$$k_2 = 0$$

$$k_3 = 0$$

$$k_4 = 0$$

$$k_5 = 0$$

will be a solution to the original system. Now we can use K to solve the original system of equations. First we will begin with the lowest order term of K and form an equation equal to zero.

$$0 = -2y^2 + x \Rightarrow x = 2y^2$$

Now we will substitute this relation into the polynomial of the basis of next highest order.

$$0 = -2xy \Rightarrow 0 = -2(2y^2)y \Rightarrow y = 0$$

Thus we can also conclude that $x = 0$, solving our system of equations. Referring back to the graph earlier in this section, you can see that the two curves intersect at the point (0,0).

4.3. Applying the Gröbner basis to our Proof

In our case this allows us to solve for the coefficients of the quadratic rational map. For the proof of Theorem 5 we use a Gröbner Basis to solve the system of equations:

$$a_2^3 - a_2 b_1^2 - 1 = 0$$

$$a_1 a_2^2 + a_1 a_2 b_1 - a_2 b_0 b_1 - a_1 b_1^2 - b_0 b_1^2 + p + q + 1 = 0$$

$$a_1^2 a_2 + a_1 a_2 b_0 + a_1^2 b_1 - a_1 b_0 b_1 - 2\, b_0^2 b_1 - pq - p - q = 0$$

$$a_1^2 b_0 - b_0^3 + pq = 0$$

$$a_2 + a_1 - b_1 - b_0 = 0$$

Note in this case a_2, a_1, b_1, b_0 are the variables and p, q are the constraints in the polynomial ring.

We form an ideal $J = \langle a_2^3 - a_2 b_1^2 - 1, a1 a_2^2 + a_1 a_2 b_1 - a_2 b_0 b_1 - a_1 b_1^2 - b_0 b_1^2 + p + q + 1,$ $a_1^2 a_2 + a_1 a_2 b_0 + a_1^2 b_1 - a_1 b_0 b_1 - 2\, b_0^2 b_1 - pq - p - q, a_1^2 b_0 - b_0^3 + pq, a_2 + a_1 - b_1 - b_0 \rangle$ from the equations and then form the Gröbner basis relative to a degrevlex ordering (see A). From this Gröbner basis we form a set of equations and solve it for the coefficients a_2, a_1, b_1, and b_0 in terms of p and q.

4.4. Uniqueness Theorem

Theorem 5. *Let p, q be distinct rational numbers. If ϕ is a quadratic rational map with fixed points 0,1, ∞ and p, q as a distinct two cycle, then ϕ is unique.*

The purpose of this proof is to solve for a_2, a_1, b_1, b_0 in terms of p, q therefore showing that they are each unique at the choice of p, q. We solve for a_2, a_1, b_1, b_0 by using the fixed point polynomials of the general second iterate of a quadratic map and the second iterate of a quadratic map with our fixed points. The fixed point polynomials establish equations in terms of a_2, a_1, b_1, b_0 and rational numbers. These equations, along with the equation obtained by requiring 1 to be a fixed point, form an ideal whose Gröbner Basis may be used to solve for the coefficients of $\phi(x)$.

Proof. We showed before that general form of a quadratic rational map fixed points 0,1, ∞ is

$$\phi(x) = \frac{a_2x^2 + a_1x}{b_1x + b_0} \text{ such that } a_2, b_0 \neq 0 \text{ and } a_2 + a_1 = b_1 + b_0$$

We will refer to $0 = a_2 + a_1 - b_1 - b_0$ as the "$\phi(1)$ equation".
The second iterate of ϕ is $\phi(\phi(x))$, given by

$$\phi(\phi(x)) = \frac{a_2(\frac{a_2x^2+a_1x}{b_1x+b_0})^2 + a_1(\frac{a_2x^2+a_1x}{b_1x+b_0})}{b_1(\frac{a_2x^2+a_1x}{b_1x+b_0}) + b_0}$$

$$= \frac{a_2^3x^4 + 2\,a_1a_2^2x^3 + a_1a_2b_1x^3 + a_1^2a_2x^2 + a_1a_2b_0x^2 + a_1^2b_1x^2 + a_1^2b_0x}{a_2b_1^2x^3 + a_2b_0b_1x^2 + a_1b_1^2x^2 + b_0b_1^2x^2 + a_1b_0b_1x + 2\,b_0^2b_1x + b_0^3}.$$

The second iterate of ϕ will maintain the fixed points 0, 1, ∞. Also the period two points p, q, will be become fixed points.

$$\phi(\phi(0)) = \phi(0) = 0$$

$$\phi(\phi(p)) = \phi(q) = p$$

The fixed point polynomial of ϕ^2 is

$$0 = a_2^3x^4 - a_2b_1^2x^4 + 2\,a_1a_2^2x^3 + a_1a_2b_1x^3 - a_2b_0b_1x^3 - a_1b_1^2x^3 - b_0b_1^2x^3$$

$$+a_1^2a_2x^2 + a_1a_2b_0x^2 + a_1^2b_1x^2 - a_1b_0b_1x^2 - 2\,b_0^2b_1x^2 + a_1^2b_0x - b_0^3x.$$

In our case, the fixed point polynomial has zeros: 0, 1, ∞, p, q.

$$0 = 1 \cdot x(x-1)(x-p)(x-q) = x^4 - px^3 - qx^3 - x^3 + pqx^2 + px^2 + qx^2 - pqx$$

Notice that $(x - \infty)$ does not appear. This is not an algebraically viable term. In order to ensure that ∞ is a fixed point, the degree of the numerator of ϕ is less than the degree of the denominator. This is achieved by ensuring that $b_2 = 0$ and $a_2 \neq 0$.

Subtracting our case from the general case, the coefficients of like terms can be combined.

$$0 = a_2^3x^4 - a_2b_1^2x^4 + 2\,a_1a_2^2x^3 + a_1a_2b_1x^3 - a_2b_0b_1x^3 - a_1b_1^2x^3 - b_0b_1^2x^3$$

$$+a_1^2a_2x^2 + a_1a_2b_0x^2 + a_1^2b_1x^2 - a_1b_0b_1x^2 - 2\,b_0^2b_1x^2 + a_1^2b_0x - b_0^3x$$

$$-(x^4 - px^3 - qx^3 - x^3 + pqx^2 + px^2 + qx^2 - pqx)$$

x^4: $a_2^3 - a_2b_1^2 - 1 = 0$

$x^3 : 2\,a_1a_2^2 + a_1a_2b_1 - a_2b_0b_1 - a_1b_1^2 - b_0b_1^2 + p + q + 1 = 0$

$x^2 : a_1^2a_2 + a_1a_2b_0 + a_1^2b_1 - a_1b_0b_1 - 2\,b_0^2b_1 - pq - p - q = 0$

$x : a_1^2b_0 - b_0^3 + pq = 0$

With the four polynomials and the $\phi(1)$ condition, we form an ideal, J, in the ring of rational polynomials with a_2, a_1, b_1, and b_0. We used Sage computer program to find the Gröbner Basis of J. From the Gröbner Basis (see Appendix A), the following equations are established:

$$a_1 + a_2 - b_0 - b_1 = 0$$

$$a_2p + a_2q - a_2 + 2b_0 + b_1 = 0$$

$$b_1pq - a_2q^2 + b_0p + a_2q - b_0q - b_1q = 0$$

From these equations the following series of dependent equations can be made.

$$b_0 = \frac{a_2pq(p+q-2)}{-2pq+p+q}$$

$$b_1 = -a_2(p+q-1) - 2b_0$$

$$a_1 = -a_2 + b_0 + b_1$$

Then when simplified all in terms of a_2

$$b_0 = \frac{a_2pq(p+q-2)}{-2pq+p+q}$$

$$b_1 = -a_2(p+q-1) - \frac{2a_2pq(p+q-2)}{-2pq+p+q}$$

$$a_1 = -a_2 - \frac{a_2pq(p+q-2)}{-2pq+p+q} - a_2(p+q-1)$$

When substituted into the general form of a quadratic rational map, refer to Theorem 3 to know that $p+q \neq 0$, $p+q-2 \neq 0$, $2pq-p-q \neq 0$. Also note that $a_2 \neq 0$.

$$\phi(x) = \frac{a_2x^2+a_1x}{b_1x+b_0} = \frac{(2pq-p-q)x^2-(p^2q+pq^2-p^2-q^2)x}{(p^2+q^2-p-q)x-pq(p+q-2)}$$

Thus $\phi(x)$ is determined unique to the two cycle p, q. □

5. General Case

5.1. Möbius Transformation

To expand our conclusions to any set of fixed points within conditions (*) from Theorem 3, we use Möbius Transformations. Below is the general form of a Möbius Transformation, and its inverse, that shifts the fixed points of the map to 0, 1, and ∞.

$$\mu(x) = \frac{(x-f_1)(f_2-f_3)}{(x-f_3)(f_2-f_1)}$$

$$f_1 \to 0$$

$$f_2 \to 1$$

$$f_3 \to \infty$$

$$\mu^{-1}(x) = \frac{f_1(f_2-f_3)-f_3x(f_2-f_1)}{f_2-f_3-x(f_2-f_1)}$$

$$f_1 \leftarrow 0$$

$$f_2 \leftarrow 1$$

$$f_3 \leftarrow \infty$$

Corollary 5.1. *Let p, q be distinct rational numbers. There is a unique quadratic rational map with fixed points f_1,f_2,f_3 and p, q as a distinct two cycle if and only if p, q satisfy the following conditions:*

$-2f_2f_3 + f_2p + f_3p + f_2q + f_3q - 2pq \neq 0$, $-2f_1f_3 + f_1p + f_3p + f_1q + f_3q - 2pq \neq 0$, $-2f_1f_2 + f_1p + f_2p + f_1q + f_2q - 2pq \neq 0$

Proof. There is a Möbius Transformation μ transforming f_1,f_2,f_3 to 0, 1, ∞.

$$\mu(x) = \frac{(x - f_1)(f_2 - f_3)}{(x - f_3)(f_2 - f_1)}$$

$$\mu^{-1}(x) = \frac{f_1(f_2 - f_3) - f_3x(f_2 - f_1)}{f_2 - f_3 - x(f_2 - f_1)}$$

This same μ also transforms transforms p, q such that: $\mu(p) + \mu(q) \neq 0$, $\mu(p) + \mu(q) - 2 \neq 0$, $2 \cdot \mu(p) \cdot \mu(q) - \mu(p) - \mu(q) \neq 0$. Once transformed, we can develop a unique quadratic rational map, as shown by Theorem 3 and Theorem 5. Then $\mu^{-1} \circ \phi \circ \mu$ is the quadratic rational map with fixed points f_1,f_2,f_3 and p, q as a distinct two cycle.

See Appendix B for the general form of a quadratic rational map with fixed points f_1,f_2,f_3 and p, q as a distinct two cycle. □

6. Affine Bijection into Moduli 2-space

Modulized spaces are used in algebraic geometry in order to translate algebraic structures, such as rational maps, into geometric structures, such as curves. The moduli 2-space, $\mathcal{M}_2$, can further be bijected into the affine plane. This provides a way by which to understand the relationships between separate maps. Via this bijection the algebraic structures correspond to single points in the two-dimensional plane. This space is described by Silverman in Chapter 4.4 of "The Arithmetic of Dynamical Systems."[3] Our work in this paper can be used to understand how these points relate to changes in fixed and period two points.

6.1. Understanding the Affine Bijection

For a proof of the isomorphism of the moduli 2-space to the affine plane, $\mathcal{M}_2 \xrightarrow{\sim} \mathbb{A}^2$, see Silverman's paper "The Space of Rational Maps on $\mathbb{P}^1$"[4]. The isomorphism is constructed using spectra dependent on multipliers. These multipliers are related to the fixed points of a quadratic rational map.

Definition 6.1. If α is a fixed point of a rational map ϕ, then the *multiplier of ϕ at α* is the derivative

$$\lambda_\alpha(\phi) = \phi'(\alpha) \ .$$

Definition 6.2. The *spectra* $\sigma_i(\phi)$ is the i^{th} elementary symmetric polynomial of the multipliers $\lambda_{\alpha_1}(\phi), \cdots, \lambda_{\alpha_{d+1}}(\phi)$. The value d is the degree of the map ϕ.

For the scope of this paper, we are concerned with the bijecion of quadratic rational maps into this space.

$$\phi \xrightarrow{\sim} (\sigma_1(\phi), \sigma_2(\phi)) \in \mathbb{A}^2$$

For a quadratic rational map, there are three fixed points and thus three multipliers.

$$\lambda_{\alpha_1}(\phi) = \phi'(\alpha_1), \lambda_{\alpha_2}(\phi) = \phi'(\alpha_2), \lambda_{\alpha_3}(\phi) = \phi'(\alpha_3)$$

These are used to construct the spectra.

$$\sigma_1(\phi) = \lambda_{\alpha_1}(\phi) + \lambda_{\alpha_2}(\phi) + \lambda_{\alpha_3}(\phi)$$

$$\sigma_2(\phi) = \lambda_{\alpha_1}(\phi)\lambda_{\alpha_2}(\phi) + \lambda_{\alpha_2}(\phi)\lambda_{\alpha_3}(\phi) + \lambda_{\alpha_2}(\phi)\lambda_{\alpha_3}(\phi)$$

6.2. Constructing Points in the Affine Plane

Continuing the trend of this paper, we will explain how this relates to a quadratic rational map with 0, 1, ∞ as fixed points.

Recall the form of a quadratic rational map with 0, 1, ∞ as fixed points and p, q for distinct two cycle.

$$\phi(x) = \frac{(2pq - p - q)x^2 - (p^2q + pq^2 - p^2 - q^2)x}{(p^2 + q^2 - p - q)x - pq(p + q - 2)}$$

The multipliers of the rational map are:

$$\lambda_0(\phi) = \frac{p^2q + pq^2 - p^2 - q^2}{p^2q + pq^2 - 2\,pq}$$

$$\lambda_1(\phi) = \frac{p^2q + pq^2 - p^2 - 4\,pq - q^2 + 2\,p + 2\,q}{p^2q + pq^2 - p^2 - 2\,pq - q^2 + p + q} + \frac{p^2 + q^2 - p - q}{p^2q + pq^2 - p^2 - 2\,pq - q^2 + p + q}\ .$$

To compute the multiplier at ∞, we change coordinates to $z = \frac{1}{x}$ and compute the multiplier at $z = 0$. This leads to the equation

$$\lambda_\infty(\phi) = \lim_{z \to\ 0} \frac{z^{-2}\phi(z^{-1})}{\phi(z^{-1})^2} = \frac{p^2 + q^2 - p - q}{2pq - p - q}\ .$$

Therefore a quadratic rational map with 0, 1, ∞ as fixed points and p, q for distinct two cycle may be sent to the affine plane with the isomorphism:

$$\mathcal{M}_2 \xrightarrow{\sim} \mathbb{A}^2$$

$$\frac{(2pq - p - q)x^2 - (p^2q + pq^2 - p^2 - q^2)x}{(p^2 + q^2 - p - q)x - pq(p + q - 2)}$$

$$\xrightarrow{\sim}$$

$$\Big(\tfrac{p^2q+pq^2-p^2-4\,pq-q^2+2\,p+2\,q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q} + \tfrac{p^2q+pq^2-p^2-q^2}{p^2q+pq^2-2\,pq} + \tfrac{p^2+q^2-p-q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q} + \tfrac{p^2+q^2-p-q}{2\,pq-p-q},$$

$$\frac{2\left(p^2q+pq^2-p^2-q^2\right)\left(\frac{p^2q+pq^2-p^2-4\,pq-q^2+2\,p+2\,q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q} + \frac{p^2+q^2-p-q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q}\right)}{p^2q+pq^2-2\,pq} + \frac{\left(p^2+q^2-p-q\right)\left(\frac{p^2q+pq^2-p^2-4\,pq-q^2+2\,p+2\,q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q} + \frac{p^2+q^2-p-q}{p^2q+pq^2-p^2-2\,pq-q^2+p+q}\right)}{2\,pq-p-q}\Big).$$

As you can see, the algebra becomes increasingly complicated. Due to the complexity of the general form with f_1, f_2, f_3 as fixed points, it is easier to take the derivative of the specific map you intend to work with to generate the multipliers and the spectra rather than provide general forms.

7. Example of Quadratic Rational Map with Two-Cycle

To bring the concepts of this paper together, we will work through an example. Let us construct the unique quadratic rational map with fixed points at 1, 2, and 3 and a two cycle of $4 \rightleftharpoons 5$.

Let's begin by making sure this is possible. Refer to the conditions of Corollary 5.1.

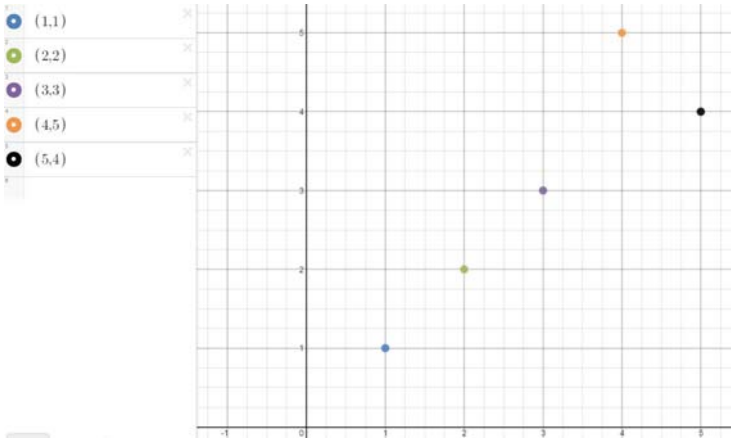
$$-2f_2f_3 + f_2p + f_3p + f_2q + f_3q - 2pq \neq 0 \Rightarrow -7 \neq 0$$

$$-2f_1f_3 + f_1p + f_3p + f_1q + f_3q - 2pq \neq 0 \Rightarrow -10 \neq 0$$

$$-2f_1f_2 + f_1p + f_2p + f_1q + f_2q - 2pq \neq 0 \Rightarrow -17 \neq 0$$

All the conditions are met. If we hold 1,2,3 as fixed points and 4 as a period 2 point, then the second period 2 point cannot be $\frac{8}{3}$, $\frac{5}{2}$, or $\frac{8}{5}$; none of which are 5. Therefore we know there exists a unique quadratic rational map with fixed points at 1, 2, and 3 and a two cycle of $4 \rightleftharpoons 5$.

Geometrically this may be visualized as constructing a curve from a quadratic function that travels through the points (1,1), (2,2), (3,3), (4,5) and (5,4).



We begin construction by bringing shifting the fixed points to 0,1, and ∞ with a Möbius Transformation.

$$\mu(x) = \frac{1-x}{x-3}$$

$$x \to \mu(x)$$

$$1 \to 0$$

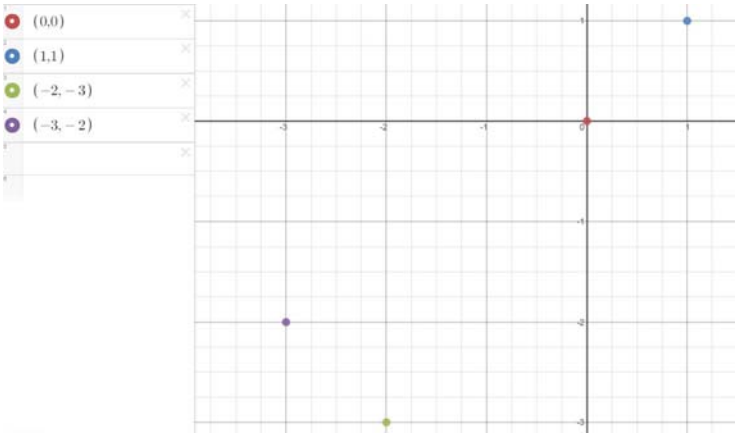
$$2 \to 1$$

$$3 \to \infty$$

$$4 \to -3$$

$$5 \to -2$$

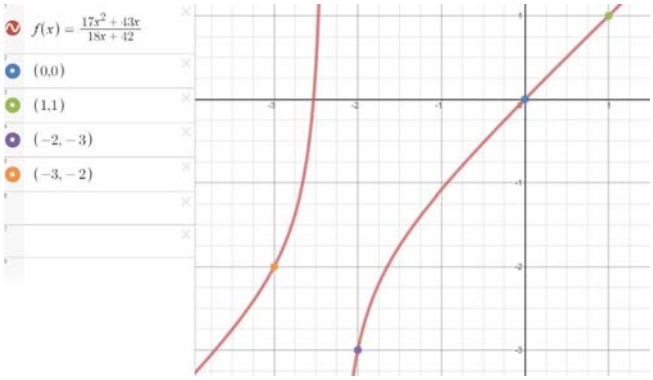
Now our visualization is shifted. We are constructing a curve that travels through the points (0,0), (1,1), the point at infinity, (-2, -3), and (-2,-3).



From here we can construct the quadratic rational map using the general form from Theorem 3.

$$(\mu(p), \mu(q)) = (-3, -2)$$

$$\phi(x) = \frac{17x^2 + 43x}{18x + 42}$$



Now we need to bring the map back to the original space. We will need the inverse Möbius Transformation.

$$\mu^{-1}(x) = \frac{1 + 3x}{1 + x}$$

$$x \leftarrow \mu^{-1}(x)$$

$$1 \leftarrow 0$$

$$2 \leftarrow 1$$

$$3 \leftarrow \infty$$

$$4 \leftarrow -3$$

$$5 \leftarrow -2$$

We can apply this to the map as a whole to bring it back to the original space.

$$\mu^{-1}(\phi(x)) = \frac{3\,(9\,x^2 - 39\,x + 2)}{x^2 + 21\,x - 106}$$

$$\phi(1) = 1$$

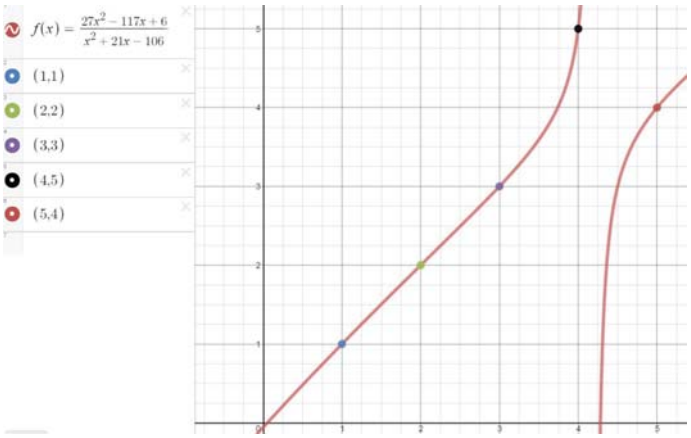
$$\phi(2) = 2$$

$$\phi(3) = 3$$

$$\phi(4) = 5$$

$$\phi(5) = 4$$

There is our unique quadratic rational map with fixed points at 1, 2, and 3 and a two cycle of $4 \rightleftharpoons 5$.



The point determined in the moduli space is then:

$$\mathcal{M}_2 \xrightarrow{\sim} \mathbb{A}^2$$

$$\frac{3\,(9\,x^2 - 39\,x + 2)}{x^2 + 21\,x - 106} \xrightarrow{\sim} \left(\frac{7297}{2380}, \frac{134173}{42840}\right)$$

8. Future Work

Definition 8.1. An *elliptic curve* $E(\mathbb{C})$ is the set of solutions (x, y) to an equation of the form

$$y^2 = x^3 + ax + b$$

together with an identity element $\mathcal{O}$. Also, it is required that $4a^3 + 27b^2 \neq 0$ which means that the cubic polynomial has distinct roots and ensures that the curve $E(\mathbb{C})$ is nonsingular.

Recently, the study of elliptic curves has grown to prominence due to their use in cryptography. Elliptic curve cyptography (ECC) is a public-key crypto-system with a smaller key length than other systems such as RSA; thereby reducing storage and transmission requirements without sacrificing security. Minimizing storage leads to increased speed and the freeing of memory towards other utility. In the end, this improves performance and saves money.

Elliptic curves are special among algebraic curves because they have a group law, i.e. a way of adding points on the curve to get another point on the curve. The group law of elliptic curves is under the operation $\oplus$ with identity point $\mathcal{O}$ [3]. By this group law, special points, known as torsion points, points develop order. The order of a point is determined by the smallest integer such that $nP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n} = 0$.

Definition 8.2. A point $P \in E$ is called a *torsion point* of order n if P has order n.

Thus you can begin to see the analogous structure of the periodic points on a rational map and the torsion points of an elliptic curve. Joseph Silverman noted the connection between these two structures in his book "Arithmetic of Dynamical Systems" [3], specifically between the subset of rational maps known as Lattès maps and elliptic curves.

Definition 8.3. A rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d \geq 2$ is called a *Lattès map* if there is an elliptic curve E, a morphism $\psi : E \to E$, and a finite separable covering $\pi : E \to \mathbb{P}^1$ such that the following diagram is commutative.

$$E \xrightarrow{\psi} E$$

$$\begin{array}{ccc} \downarrow^{\pi} & & \downarrow^{\pi} \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

For example, let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let ψ be the duplication map such that $\psi(P) = P \oplus P = 2P$ and $\pi(P) = \pi(x, y) = x$. Then the related Lattès map is [3]

$$\phi_E(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

When maps have higher degree than two, they develop a larger set of interesting points which encompasses fixed and periodic points. This larger set is the map's pre-periodic points.

Definition 8.4. Let α be a point on the projective line $\mathbb{P}^1$ and let n and m be distinct integers such that

$$\phi^m(\alpha) = \phi^n(\alpha)$$

The point α is known as a *pre-periodic point*, denoted PrePer(ϕ). Note that all periodic points are pre-periodic points.

It is in these points that Silverman proved the connection of rational maps to elliptic curves.

Theorem 6. *Let ϕ be a Lattès map associated to an elliptic curve E. Then*

$$PrePer(\phi) = \pi(E_{tor})$$

It is this connection that our research seeks to exploit.

Our current work capitalizes upon simpler calculations in the space of quadratic rational maps with fixed points $0, 1, \infty$ than the space of elliptic curves. We then transform our construction to the desired space of fixed points f_1, f_2, f_3. We can do this by exploiting the fact that Möbius transformations exists between any three distinct triples.

Future work would use an analogous bait and switch. We would work in the space of Lattès maps with certain pre-periodic points. We would then transform our construction to the desired space of elliptic curves with certain torsion points. We do this by exploiting the above theorem by Silverman.

This algorithm of construction could then be an asset for generating new keys in elliptic curve cryptography.

A. Gröbner Basis of the Ideal

$$b_0^3p^2+\tfrac{1}{8}b_1^3p^2-2b_0^3pq+b_0^3q^2-\tfrac{7}{4}a_2b_1^2q^2-4b_0b_1^2q^2-\tfrac{15}{8}b_1^3q^2-\tfrac{1}{2}p^3q^2-\tfrac{1}{2}p^2q^3-\tfrac{1}{8}b_1^3p+2a_2^2b_1q-8b_0^2b_1q-\tfrac{1}{4}a_2b_1^2q-\tfrac{15}{2}b_0b_1^2q-\tfrac{15}{8}b_1^3q-\tfrac{1}{4}p^3q+\tfrac{3}{2}p^2q^2-\tfrac{1}{4}pq^3-4b_0^3-\tfrac{1}{2}a_2^2b_1-4b_0^2b_1+\tfrac{1}{8}a_2b_1^2-\tfrac{1}{4}b_0b_1^2+\tfrac{3}{8}b_1^3-\tfrac{1}{8}p^3+\tfrac{5}{8}p^2q-\tfrac{11}{8}pq^2+\tfrac{15}{8}q^3+\tfrac{1}{4}p^2+\tfrac{3}{4}pq-\tfrac{7}{4}q^2-\tfrac{5}{8}p-\tfrac{5}{8}q+\tfrac{1}{2},\ a_2b_0b_1q^2+\tfrac{1}{2}a_2b_1^2q^2+b_0b_1^2q^2+\tfrac{1}{2}b_1^3q^2-\tfrac{1}{2}a_2^2b_1q-a_2b_0b_1q+4b_0^2b_1q+3b_0b_1^2q+\tfrac{1}{2}b_1^3q+2b_0^3+\tfrac{1}{4}a_2^2b_1+\tfrac{1}{2}a_2b_0b_1+b_0^2b_1-\tfrac{1}{2}b_0b_1^2-\tfrac{1}{4}b_1^3+\tfrac{1}{2}pq^2-\tfrac{1}{2}q^3-\tfrac{1}{2}pq+\tfrac{1}{2}q^2+\tfrac{1}{4}p+\tfrac{1}{4}q-\tfrac{1}{4},\ b_0^2b_1q^2+\tfrac{1}{4}a_2b_1^2q^2+b_0b_1^2q^2+\tfrac{1}{4}b_1^3q^2-\tfrac{1}{2}b_0^3p-\tfrac{1}{16}b_1^3p+\tfrac{3}{2}b_0^3q+\tfrac{1}{2}a_2b_0b_1q+2b_0^2b_1q+\tfrac{1}{2}b_0b_1^2q-\tfrac{1}{16}b_1^3q+\tfrac{1}{4}p^2q^2+\tfrac{1}{2}pq^3+b_0^3+\tfrac{3}{16}a_2^2b_1+\tfrac{1}{8}a_2b_0b_1+\tfrac{1}{2}b_0^2b_1-\tfrac{1}{16}a_2b_1^2-\tfrac{1}{4}b_0b_1^2-\tfrac{1}{8}b_1^3+\tfrac{1}{8}p^2q-\tfrac{5}{8}pq^2-\tfrac{1}{4}q^3+\tfrac{1}{16}p^2-\tfrac{1}{8}pq+\tfrac{9}{16}q^2+\tfrac{1}{16}p-\tfrac{3}{16}q-\tfrac{1}{8},\ b_0^2b_1p-\tfrac{1}{4}b_1^3p+b_0^2b_1q-\tfrac{1}{4}b_1^3q+2b_0^3+\tfrac{1}{2}a_2^2b_1+\tfrac{1}{2}a_2b_0b_1-\tfrac{1}{4}a_2b_1^2-b_0b_1^2-\tfrac{1}{4}b_1^3+\tfrac{1}{2}p^2q+\tfrac{1}{2}pq^2+\tfrac{1}{4}p^2-pq+\tfrac{1}{4}q^2-\tfrac{1}{4},\ b_0b_1^2p+\tfrac{1}{2}b_1^3p+b_0b_1^2q+\tfrac{1}{2}b_1^3q-\tfrac{1}{2}a_2^2b_1+2b_0^2b_1+\tfrac{1}{2}a_2b_1^2+b_0b_1^2-\tfrac{1}{2}p^2-\tfrac{1}{2}q^2+\tfrac{1}{2}p+\tfrac{1}{2}q,\ a_2^2q^2+a_2b_1q^2-a_2^2q+2a_2b_0q+2b_0b_1q+b_1^2q-a_2b_0+2b_0^2+b_0b_1,\ a_2^3-a_2b_1^2-1,\ a_2^2b_0+\tfrac{1}{2}a_2^2b_1-b_0b_1^2-\tfrac{1}{2}b_1^3+\tfrac{1}{2}p+\tfrac{1}{2}q-\tfrac{1}{2},\ a_2b_0^2+\tfrac{1}{4}a_2^2b_1+a_2b_0b_1-b_0^2b_1-b_0b_1^2-\tfrac{1}{4}b_1^3-\tfrac{1}{2}pq+\tfrac{1}{4}p+\tfrac{1}{4}q-\tfrac{1}{4},\ b_1pq-a_2q^2+b_0p+a_2q-b_0q-b_1q,\ a_2p+a_2q-a_2+2b_0+b_1,\ a_1+a_2-b_0-b_1$$

B. Proof of Corollary without Transformation

Let f_1,f_2,f_3, p and q be distinct rational numbers.
Let $S = \{\ \frac{(f_1-f_2)f_3p-f_1f_2+f_1f_3}{(f_1-f_2)p-f_2+f_3}, \frac{(f_1-f_2)f_3(p-2)-f_1f_2+f_1f_3}{(f_1-f_2)(p-2)-f_2+f_3}, \frac{f_1f_2-f_1f_3+\frac{(f_1-f_2)f_3p}{2p-1}}{f_2-f_3+\frac{(f_1-f_2)p}{2p-1}}\ \}$.
Given any 3 fixed points (f_1,f_2,f_3) and any other pair of points (p,q) such that $q \notin S$, there is exactly 1 rational map with the 3 fixed points and with the other pair of points forming a two-cycle.

Proof. The map is given by:

$$\phi(x) = (f_1f_2f_3p^2-2\,f_1f_2f_3pq+f_1f_2f_3q^2+f_1f_2f_3px-f_1f_2p^2x-f_1f_3p^2x-f_2f_3p^2x+f_1f_2f_3qx+f_1p^2qx+f_2p^2qx+f_3p^2qx-f_1f_2q^2x-f_1f_3q^2x-f_2f_3q^2x+f_1pq^2x+f_2pq^2x+f_3pq^2x-2\,p^2q^2x-2\,f_1f_2f_3x^2+f_1f_2px^2+f_1f_3px^2+f_2f_3px^2+f_1f_2qx^2+f_1f_3qx^2+f_2f_3qx^2-2\,f_1pqx^2-2\,f_2pqx^2-2\,f_3pqx^2+p^2qx^2+pq^2x^2)\cdot(f_1f_2f_3p+f_1f_2f_3q-2\,f_1f_2pq-2\,f_1f_3pq-2\,f_2f_3pq+f_1p^2q+f_2p^2q+f_3p^2q+f_1pq^2+f_2pq^2+f_3pq^2-2\,p^2q^2-2\,f_1f_2f_3x+f_1f_2px+f_1f_3px+f_2f_3px-f_1p^2x-f_2p^2x-f_3p^2x+f_1f_2qx+f_1f_3qx+f_2f_3qx+p^2qx-f_1q^2x-f_2q^2x-f_3q^2x+pq^2x+p^2x^2-2\,pqx^2+q^2x^2)^{-1}$$

If $f(f_1) = f_1$, $f(f_2) = f_2$, $f(f_3) = f_3$, then f_1,f_2,f_3 are fixed points.

$$f(f_1) = (2\,f_1^3f_2f_3-f_1^3f_2p-f_1^3f_3p-2\,f_1^2f_2f_3p+f_1^2f_2p^2+f_1^2f_3p^2-f_1^3f_2q-f_1^3f_3q-2\,f_1^2f_2f_3q+2\,f_1^3pq+2\,f_1^2f_2pq+2\,f_1^2f_3pq+2\,f_1f_2f_3pq-2\,f_1^2p^2q-f_1f_2p^2q-f_1f_3p^2q+f_1^2f_2q^2+f_1^2f_3q^2-2\,f_1^2pq^2-f_1f_2pq^2-f_1f_3pq^2+2\,f_1p^2q^2)\cdot(2\,f_1^2f_2f_3-f_1^2f_2p-f_1^2f_3p-2\,f_1f_2f_3p+f_1f_2p^2+f_1f_3p^2-f_1^2f_2q-f_1^2f_3q-2\,f_1f_2f_3q+2\,f_1^2pq+2\,f_1f_2pq+2\,f_1f_3pq+2\,f_2f_3pq-2\,f_1p^2q-f_2p^2q-f_3p^2q+f_1f_2q^2+f_1f_3q^2-2\,f_1pq^2-f_2pq^2-f_3pq^2+2\,p^2q^2)^{-1}$$

$$= f_1\cdot(2\,f_1^2f_2f_3-f_1^2f_2p-f_1^2f_3p-2\,f_1f_2f_3p+f_1f_2p^2+f_1f_3p^2-f_1^2f_2q-f_1^2f_3q-2\,f_1f_2f_3q+2\,f_1^2pq+2\,f_1f_2pq+2\,f_1f_3pq+2\,f_2f_3pq-2\,f_1p^2q-f_2p^2q-f_3p^2q+f_1f_2q^2+f_1f_3q^2-2\,f_1pq^2-f_2pq^2-f_3pq^2+2\,p^2q^2)\cdot(2\,f_1^2f_2f_3-f_1^2f_2p-f_1^2f_3p-2\,f_1f_2f_3p+f_1f_2p^2+f_1f_3p^2-f_1^2f_2q-f_1^2f_3q-2\,f_1f_2f_3q+2\,f_1^2pq+2\,f_1f_2pq+2\,f_1f_3pq+2\,f_2f_3pq-2\,f_1p^2q-f_2p^2q-f_3p^2q+f_1f_2q^2+f_1f_3q^2-2\,f_1pq^2-f_2pq^2-f_3pq^2+2\,p^2q^2)^{-1}$$

$= f_1$

$f(f_2) = (2\,f_1 f_2^3 f_3 - f_1 f_2^3 p - 2\,f_1 f_2^2 f_3 p - f_2^3 f_3 p + f_1 f_2^2 p^2 + f_2^2 f_3 p^2 - f_1 f_2^3 q - 2\,f_1 f_2^2 f_3 q - f_2^3 f_3 q + 2\,f_1 f_2^2 pq + 2\,f_2^3 pq + 2\,f_1 f_2 f_3 pq + 2\,f_2^2 f_3 pq - f_1 f_2 p^2 q - 2\,f_2^2 p^2 q - f_2 f_3 p^2 q + f_1 f_2^2 q^2 + f_2^2 f_3 q^2 - f_1 f_2 pq^2 - 2\,f_2^2 pq^2 - f_2 f_3 pq^2 + 2\,f_2 p^2 q^2) \cdot (2\,f_1 f_2^2 f_3 - f_1 f_2^2 p - 2\,f_1 f_2 f_3 p - f_2^2 f_3 p + f_1 f_2 p^2 + f_2 f_3 p^2 - f_1 f_2^2 q - 2\,f_1 f_2 f_3 q - f_2^2 f_3 q + 2\,f_1 f_2 pq + 2\,f_2^2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq - f_1 p^2 q - 2\,f_2 p^2 q - f_3 p^2 q + f_1 f_2 q^2 + f_2 f_3 q^2 - f_1 pq^2 - 2\,f_2 pq^2 - f_3 pq^2 + 2\,p^2 q^2)^1$

$= f_2 \cdot (2\,f_1 f_2^2 f_3 - f_1 f_2^2 p - 2\,f_1 f_2 f_3 p - f_2^2 f_3 p + f_1 f_2 p^2 + f_2 f_3 p^2 - f_1 f_2^2 q - 2\,f_1 f_2 f_3 q - f_2^2 f_3 q + 2\,f_1 f_2 pq + 2\,f_2^2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq - f_1 p^2 q - 2\,f_2 p^2 q - f_3 p^2 q + f_1 f_2 q^2 + f_2 f_3 q^2 - f_1 pq^2 - 2\,f_2 pq^2 - f_3 pq^2 + 2\,p^2 q^2) \cdot (2\,f_1 f_2^2 f_3 - f_1 f_2^2 p - 2\,f_1 f_2 f_3 p - f_2^2 f_3 p + f_1 f_2 p^2 + f_2 f_3 p^2 - f_1 f_2^2 q - 2\,f_1 f_2 f_3 q - f_2^2 f_3 q + 2\,f_1 f_2 pq + 2\,f_2^2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq - f_1 p^2 q - 2\,f_2 p^2 q - f_3 p^2 q + f_1 f_2 q^2 + f_2 f_3 q^2 - f_1 pq^2 - 2\,f_2 pq^2 - f_3 pq^2 + 2\,p^2 q^2)^{-1}$

$= f_2$

$f(f_3) = (2\,f_1 f_2 f_3^3 - 2\,f_1 f_2 f_3^2 p - f_1 f_3^3 p - f_2 f_3^3 p + f_1 f_3^2 p^2 + f_2 f_3^2 p^2 - 2\,f_1 f_2 f_3^2 q - f_1 f_3^3 q - f_2 f_3^3 q + 2\,f_1 f_2 f_3 pq + 2\,f_1 f_3^2 pq + 2\,f_2 f_3^2 pq + 2\,f_3^3 pq - f_1 f_3 p^2 q - f_2 f_3 p^2 q - 2\,f_3^2 p^2 q + f_1 f_3^2 q^2 + f_2 f_3^2 q^2 - f_1 f_3 pq^2 - f_2 f_3 pq^2 - 2\,f_3^2 pq^2 + 2\,f_3 p^2 q^2) \cdot (2\,f_1 f_2 f_3^2 - 2\,f_1 f_2 f_3 p - f_1 f_3^2 p - f_2 f_3^2 p + f_1 f_3 p^2 + f_2 f_3 p^2 - 2\,f_1 f_2 f_3 q - f_1 f_3^2 q - f_2 f_3^2 q + 2\,f_1 f_2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq + 2\,f_3^2 pq - f_1 p^2 q - f_2 p^2 q - 2\,f_3 p^2 q + f_1 f_3 q^2 + f_2 f_3 q^2 - f_1 pq^2 - f_2 pq^2 - 2\,f_3 pq^2 + 2\,p^2 q^2)^1$

$= f_3 \cdot (2\,f_1 f_2 f_3^2 - 2\,f_1 f_2 f_3 p - f_1 f_3^2 p - f_2 f_3^2 p + f_1 f_3 p^2 + f_2 f_3 p^2 - 2\,f_1 f_2 f_3 q - f_1 f_3^2 q - f_2 f_3^2 q + 2\,f_1 f_2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq + 2\,f_3^2 pq - f_1 p^2 q - f_2 p^2 q - 2\,f_3 p^2 q + f_1 f_3 q^2 + f_2 f_3 q^2 - f_1 pq^2 - f_2 pq^2 - 2\,f_3 pq^2 + 2\,p^2 q^2) \cdot (2\,f_1 f_2 f_3^2 - 2\,f_1 f_2 f_3 p - f_1 f_3^2 p - f_2 f_3^2 p + f_1 f_3 p^2 + f_2 f_3 p^2 - 2\,f_1 f_2 f_3 q - f_1 f_3^2 q - f_2 f_3^2 q + 2\,f_1 f_2 pq + 2\,f_1 f_3 pq + 2\,f_2 f_3 pq + 2\,f_3^2 pq - f_1 p^2 q - f_2 p^2 q - 2\,f_3 p^2 q + f_1 f_3 q^2 + f_2 f_3 q^2 - f_1 pq^2 - f_2 pq^2 - 2\,f_3 pq^2 + 2\,p^2 q^2)^{-1}$

$= f_3$

Therefore it is shown that f_1,f_2,f_3 are fixed points.
If $f(p) = q$ and $f(q) = p$, then p, q form a two cycle.

$f(p) = (f_1f_2f_3pq - f_1f_2p^2q - f_1f_3p^2q - f_2f_3p^2q + f_1p^3q + f_2p^3q + f_3p^3q - p^4q - f_1f_2f_3q^2 + f_1f_2pq^2 + f_1f_3pq^2 + f_2f_3pq^2 - f_1p^2q^2 - f_2p^2q^2 - f_3p^2q^2 + p^3q^2) \cdot (f_1f_2f_3pq - f_1f_2p^2q - f_1f_3p^2q - f_2f_3p^2q + f_1p^3q + f_2p^3q + f_3p^3q - p^4q - f_1f_2f_3q^2 + f_1f_2pq^2 + f_1f_3pq^2 + f_2f_3pq^2 - f_1p^2q^2 - f_2p^2q^2 - f_3p^2q^2 + p^3q^2)^{-1}$

$= q \cdot (f_1f_2f_3pq - f_1f_2p^2q - f_1f_3p^2q - f_2f_3p^2q + f_1p^3q + f_2p^3q + f_3p^3q - p^4q - f_1f_2f_3q^2 + f_1f_2pq^2 + f_1f_3pq^2 + f_2f_3pq^2 - f_1p^2q^2 - f_2p^2q^2 - f_3p^2q^2 + p^3q^2) \cdot (f_1f_2f_3pq - f_1f_2p^2q - f_1f_3p^2q - f_2f_3p^2q + f_1p^3q + f_2p^3q + f_3p^3q - p^4q - f_1f_2f_3q^2 + f_1f_2pq^2 + f_1f_3pq^2 + f_2f_3pq^2 - f_1p^2q^2 - f_2p^2q^2 - f_3p^2q^2 + p^3q^2)^{-1}$

$= q$

$f(q) = (f_1f_2f_3p^2 - f_1f_2f_3pq - f_1f_2p^2q - f_1f_3p^2q - f_2f_3p^2q + f_1f_2pq^2 + f_1f_3pq^2 + f_2f_3pq^2 + f_1p^2q^2 + f_2p^2q^2 + f_3p^2q^2 - f_1pq^3 - f_2pq^3 - f_3pq^3 - p^2q^3 + pq^4) \cdot (f_1f_2f_3p - f_1f_2f_3q - f_1f_2pq - f_1f_3pq - f_2f_3pq + f_1f_2q^2 + f_1f_3q^2 + f_2f_3q^2 + f_1pq^2 + f_2pq^2 + f_3pq^2 - f_1q^3 - f_2q^3 - f_3q^3 - pq^3 + q^4)^{-1}$

$= p \cdot (f_1f_2f_3p - f_1f_2f_3q - f_1f_2pq - f_1f_3pq - f_2f_3pq + f_1f_2q^2 + f_1f_3q^2 + f_2f_3q^2 + f_1pq^2 + f_2pq^2 + f_3pq^2 - f_1q^3 - f_2q^3 - f_3q^3 - pq^3 + q^4) \cdot (f_1f_2f_3p - f_1f_2f_3q - f_1f_2pq - f_1f_3pq - f_2f_3pq + f_1f_2q^2 + f_1f_3q^2 + f_2f_3q^2 + f_1pq^2 + f_2pq^2 + f_3pq^2 - f_1q^3 - f_2q^3 - f_3q^3 - pq^3 + q^4)^{-1}$

$= p$

Thus p, q form a two-cycle for $f(x)$.

□

C. SageMath Construction Function for a Quadratic Rational Map

```
def affine_bijection(f1,f2,f3,p,q):
    #This function will produce the affine bijection of a given rational map
    #f1, f2, and f3 are the fixed points
    #p, q are the two-cycle
    #Note: if after the mobius transformation q=(-p)/(1-2*p), then there is
     no map
    #Note: if q=imt(-mt(p)/(1-2*mt(p)))=
     (f1*f2 - f1*f3 + (f1 - p)*(f2 - f3)*f3/((f3 - p)*(2*(f1 - p)*(f2 - f3)/
     ((f1 - f2)*(f3 - p)) + 1)))/(f2 - f3 +
     (f1 - p)*(f2 - f3)/((f3 - p)*(2*(f1 - p)*(f2 - f3)/
     ((f1 - f2)*(f3 - p)) + 1))) then there is no map
    #By a mobius transformation, f1 will shift to 0, f2 will shift to 1,
     and f3 will shift to infinity
    z=var('z')
    def mobius_tansformation(z1,z2,z3):
        return ((z-z1)*(z2-z3))/((z-z3)*(z2-z1))
    def inverse_mobius_transformation(z1,z2,z3):
        return (z1*(z2-z3)-z3*z*(z2-z1))/(z2-z3-z*(z2-z1))
    mt(z)=mobius_tansformation(f1,f2,f3)
    imt(z)=inverse_mobius_transformation(f1,f2,f3)
    p=mt(p)
    q=mt(q)
    #Next line is optional way of intstituting the interesting point,
     the map is actually developed
    #q=(-p)/(1-2*p)
    #P and q are currently symbolic expressions, the need to be coerced
     to rationals
    p=QQ(p)
    q=QQ(q)
```

```
#p,q is the two-cylce pair, the other fixed points have been moved
 to 0,1, and infinity
A.<a0,a1,a2,b0,b1,b2>=QQ[];
P.<X,Y>=ProjectiveSpace(A,1);
#H is the space of all rational maps from this projective space to itself.
H = Hom(P,P);
#After doing the algebra of the Groebner basis of the second iterate map,
 the coeficients have been distilled to:
a2=-( p + q - 2*p*q)
#b0= a2*(p*q)*(p+q-2)/(p + q - 2*p*q)
#Below is b0 simplified. What this allows is to develop maps
 where q=imt(-mt(p)/(1-2*mt(p)))
b0= -(p*q)*(p+q-2)
b1= -a2*(p+q-1) - 2*b0
a1= -a2 + b1 + b0
#return p and q to original values
p=imt(p)
q=imt(q)
#Create the Rational Map
P1.<X,Y>=ProjectiveSpace(QQ,1);
U=Hom(P1,P1)
#The fuction m is developed by doing the inverse mobius transformation
of the map with a2, a2, b1, b0 as the coefficients
c0=-b0*f1^2 + b0*f1*f2 + b1*f1*f2 + a1*f1*f3 - b1*f1*f3 - a1*f2*f3
 - a2*f2*f3 + a2*f3^2
c1= -b1*f1^2*f2 - a1*f1^2*f3 + 2*b0*f1^2*f3 + b1*f1^2*f3 + a1*f1*f2*f3
 + 2*a2*f1*f2*f3 - 2*b0*f1*f2*f3 - b1*f1*f2*f3 - a1*f1*f3^2
 - 2*a2*f1*f3^2 + b1*f1*f3^2 + a1*f2*f3^2
c2= -a2*f1^2*f2*f3 + b1*f1^2*f2*f3 + a1*f1^2*f3^2 + a2*f1^2*f3^2
- b0*f1^2*f3^2 - b1*f1^2*f3^2 - a1*f1*f2*f3^2 + b0*f1*f2*f3^2
```

```
    d0=a1*f1 - b0*f1 - a1*f2 - a2*f2 + b0*f2 + b1*f2 + a2*f3 - b1*f3
    d1=-a1*f1^2 + a1*f1*f2 + 2*a2*f1*f2 - b1*f1*f2 - a1*f1*f3 - 2*a2*f1*f3
    + 2*b0*f1*f3 + b1*f1*f3 + a1*f2*f3 - 2*b0*f2*f3 - b1*f2*f3 + b1*f3^2
    d2=-a2*f1^2*f2 + a1*f1^2*f3 + a2*f1^2*f3 - a1*f1*f2*f3 + b1*f1*f2*f3
    - b0*f1*f3^2 - b1*f1*f3^2 + b0*f2*f3^2
    m=U([((X^2)*c0+(Y*X)*c1+ (Y^2)*c2), ((X^2)*d0+ (X*Y)*d1 + (Y^2)*d2)]);
    E=[[' ', f1, f2, f3, p, q],['f(x)',m(f1,1)[0]/m(f1,1)[1],
     m(f2,1)[0]/m(f2,1)[1],f3,m(p,1)[0]/m(p,1)[1],m(q,1)[0]/m(q,1)[1]],
     ['f(f(X))', m(m(f1,1)[0]/m(f1,1)[1],1)[0]/m(m(f1,1)[0]/m(f1,1)[1],1)
     [1], m(m(f2,1)[0]/m(f2,1)[1],1)[0]/m(m(f2,1)[0]/m(f2,1)[1],1)[1],
     f3,m(m(p,1)[0]/m(p,1)[1],1)[0]/m(m(p,1)[0]/m(p,1)[1],1)[1],
     m(m(q,1)[0]/m(q,1)[1],1)[0]/m(m(q,1)[0]/m(q,1)[1],1)[1]]]
    #f(x) is the rational map with fixed points f1, f2, f3 and two cycle p,q
    f(x)=((x^2)*c0+(x)*c1+ c2)/ ((x^2)*d0+ (x)*d1 + d2)
    L1(x)=diff(f(x),x)
    L2(x)=diff(f(x),x)
    L3(x)=diff(f(x),x)
    Sig1=L1(f1)+L2(f2)+L3(f3)
    Sig2=L1(f1)*L2(f2)+L2(f2)*L3(f3)+L1(f1)*L3(f3)
    return show((f1,f2,f3,p,q), '===>' ,f(x),
    '===>', (Sig1,Sig2)), table(E, frame=True)
```

```
affine_bijection(1,2,3,4,5)
```

$(1,2,3,4,5)$ ===> $\frac{3\left(9x^2-39x+2\right)}{x^2+21x-106}$ ===> $\left(\frac{7297}{2380}\ \frac{134173}{42840}\right)$

x	1	2	3	4	5
f(x)	1	2	3	5	4
f(f(x))	1	2	3	4	5

D. References

[1] K. Cirdwell, S. Gilbertson, N. Nuechterlein, K. Pilgrim, and S. Pinella. On the Classification of Critically Fixed Maps. *Conformal Geometry and Dynamics*, 2013.

[2] David Cox, John Little, Donal O'Shea *Ideals, Varieties, and Algorithms*. Springer, 2000, ISBN: 978-0-387-35650-1

[3] Joseph H. Silverman *Arithmetic of Dynamical Systems.* Graduate Texts in Mathematics. Springer, 2007, ISBN: 978-0-387-69906-5.

[4] Joseph H. Silverman. The Space of Rational Maps on $\mathbb{P}^1$. *Duke Math Journal*, 1998.